ROB BONTA
Attorney General of California
ANYA M. BINSACCA, State Bar No. 189613
Supervising Deputy Attorney General
KRISTIN A. LISKA, State Bar No. 315994
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3916
Fax: (415) 703-5480
E-mail: Kristin.Liska@doj.ca.gov
Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

SACRAMENTO DIVISION

CHRISTOPHER KOHLS, et al., Plaintiffs, **v.** **ROB BONTA, in His Official Capacity as Attorney General of the State of California, and SHIRLEY N. WEBER, in Her Official Capacity as California Secretary of State,** Defendants.	Case No. 2:24-cv-02527-JAM-CKD **DEFENDANTS' STATEMENT OF UNDISPUTED FACTS** Date: August 5, 2025 Time: 1:00 p.m. Dept: 6 Judge: The Honorable John A. Mendez Trial Date: Not Scheduled Action Filed: 9/17/2024

I. BACKGROUND ON THE PARTIES

1. Plaintiff Christopher Kohls creates humorous content satirizing political figures under the screenname "Mr. Reagan." *Kohls* Compl. [ECF No. 1] ¶¶ 4, 17.

2. His content includes a video depicting then-candidate Kamala Harris that intersperses actual speeches she gave with digitally created audio. *Kohls* Compl. ¶¶ 5-6, 33.

3. This video was shared on the platform X by Elon Musk and garnered over 100 million views. Elon Musk's post did not note that the video was a satire or parody. *Kohls* Compl. ¶ 8.

4. Plaintiff The Babylon Bee is a Florida company that publishes satirical news articles, photographs, and videos on its own website and its social media accounts. These include satirical articles, photographs, and videos on political subjects. The Babylon Bee's followers include California residents. *Babylon Bee* Compl. [ECF No. 21] ¶¶ 10-12, 41-43, 47, 52-54, 57-58, 60-62.

5. Plaintiff Kelly Chang Rickert is a California resident who publishes about topics such as politics, elections, and culture on her blog and social media accounts. Her readers and subscribers include California residents. *Babylon Bee* Compl. ¶¶ 13, 110-111, 113, 115-116.

6. Plaintiff Rumble Canada is the owner and operator of Rumble, an online video-sharing platform. *Rumble* Compl. [ECF No. 33] ¶¶ 2, 9-10, 19-20.

7. Plaintiff Rumble, Inc. is the owner of Rumble Canada. *Rumble* Compl. ¶ 9.

8. Plaintiff X Corp. is the operator of the X service, a social media platform that allows users to post and distribute content for other users to interact with. *X Corp.* Compl. [ECF No. 38] ¶ 21.

9. Defendant Attorney General Rob Bonta is the chief law enforcement officer of California and is tasked with enforcing state laws. He is sued in his official capacity. *See* Cal. Const. Art. V, § 13.

10. Defendant Secretary of State Shirley N. Weber is the chief elections officer of California. She is sued in her official capacity. *See* Cal. Elec. Code § 10(a).

II. BACKGROUND ON POLITICAL DEEPFAKES

11. Visual representations of candidates are influential on voters in deciding which candidate to vote for. Alvarez Decl. ¶¶ 5, 46.

12. Candidates, campaigns, and others can manipulate visual representations to impact voter turnout or decision-making. Alvarez Decl. ¶¶ 6, 47.

13. Historically this manipulation was done with non-synthetic or traditional technologies such as the software Adobe Photoshop. Many tools for detecting non-synthetic manipulated visual images have been created. Alvarez Decl. ¶ 7.

14. Modern technology such as artificial intelligence can now be used for the synthetic manipulation of visual or video media. Such technology can create very realistic manipulated content that can be increasingly difficult to detect. It can also do so very quickly, sometimes in only a matter of seconds. Some of this technology can be found freely available for download online. Alvarez Decl. ¶¶ 8-9, 18-19, 30-32, 48.

15. Deepfakes are synthetically altered digital content that has been manipulated to deceptively claim or imply that an event or statement occurred that did not in fact occur. Alvarez Decl. ¶ 8.

16. Modern deepfakes are increasingly difficult to detect as technology has evolved to make it easier to produce more sophisticated deepfakes. In addition, as tools and algorithms develop to detect deepfakes, those same tools can be used to create better, more effective, and more difficult to detect deepfakes. Alvarez Decl. ¶¶ 18-19, 30-32, 48-49, 52.

17. Political deepfakes are an existing concern for elections. One database, the Political Deepfakes Incidents Database, contains over 800 reported political deepfake incidents. This is likely an underestimate of the number of disseminated political deepfakes. An example of political deepfakes includes a video manipulated to depict President Trump kissing Elon Musk’s feet that was distributed via hacked screens at the U.S. Department of Housing and Urban Development’s headquarters. Alvarez Decl. ¶ 10, 21.

19. Other examples of potential political deepfakes include a digitally created video of former President Joe Biden announcing the beginning of World War III and the draft, digitally

created photos of then-former President Donald Trump being arrested, manipulated photos of then-former President Trump embracing Dr. Anthony Fauci, and digitally created robocalls allegedly from former President Joe Biden placed to New Hampshire voters telling them not to vote in the 2024 New Hampshire primary election. Liska Decl., Exs. 14-19.

18. Political deepfakes pose a risk of harm to democracy. They can manipulate voters to change their opinion, attitude, or preference on who to vote for or whether to vote and can sow confusion that impacts voting behavior. They can generate distrust in political institutions and electoral procedures. They can spread misinformation about election rules and procedures. And they can lead to harassment of election officials and workers and thus to interference in the electoral process. Alvarez Decl. ¶¶ 10-17, 28- 29, 47, 50.

19. Political deepfakes also pose a national security threat. Evidence has indicated that foreign actors, including China and Russia, have made active attempts to manipulate American public opinion and events through the use of deceptive misinformation. Alvarez Decl. ¶¶ 35-37, 51.

20. Political deepfakes can spread rapidly online and can spread faster, farther, and deeper than truthful content. This is particularly true with deepfakes or misinformation targeted to specific audiences. Alvarez Decl. ¶¶ 25-28, 49.

21. Political deepfakes can also spread via networks that are harder to monitor or access, such as encrypted messaging applications, private social media groups, or personalized content delivery systems. Such networks can remain largely invisible to researchers, platform governance teams, and electoral oversight bodies. Alvarez Decl. ¶¶ 26-28, 33.

22. Multiple factors make it difficult to detect political deepfakes online, including advances in technology that make deepfakes harder to detect and the online environment where they are distributed. Alvarez Decl. ¶¶ 26-28, 30-34, 49, 52.

23. Political deepfakes are "sticky." They have persistent impacts on viewers, even when viewers are aware that the video is a deepfake. This can be especially true for deepfakes targeted towards a particular audience. Alvarez Decl. ¶¶ 22-24, 28-29, 39, 53.

24. There are two strategies to mitigate the impact of political deepfakes, pre-bunking and de-bunking. Either would require a large investment of resources and it is unclear how they could be deployed at a large scale such as the state of California. Alvarez Decl. ¶ 38, 40, 54.

25. Pre-bunking involves exposing individuals to misinformation and warning in advance that it is misinformation. To be an effective mitigation strategy, it requires identifying a deepfake's message prior to distribution and undertaking a population-wide effort to warn potential viewers in advance. Alvarez Decl. ¶¶ 38-39.

26. De-bunking involves trying to persuade an individual that misinformation is incorrect after exposure. To be an effective mitigation strategy, it requires targeting all or most viewers of a deepfake once it has been distributed and providing them with effective counter-messaging. Research has indicated, however, that once misinformation takes hold it can continue to mislead a viewer even after being debunked. Alvarez Decl. ¶¶ 38-39.

III. BACKGROUND ON AB 2655 AND AB 2839

27. AB 2655 and AB 2839 were enacted to further California's compelling interest in protecting free and fair elections. Cal. Elec. Code §§ 20012(a)(4), 20511(e)

28. In enacting AB 2655 and AB 2839, the Legislature found that "[i]n order to ensure California elections are free and fair, California must, for a limited time before and after elections, prevent the use of deepfakes and disinformation meant to prevent voters from voting and deceive voters based on fraudulent content." Cal Elec. Code §§ 20012(a)(4), 200511(e).

29. The Legislature found that "bad actors now have the power to create a false image of a candidate accepting a bribe, or a fake video of an elections official 'caught on tape' saying that voting machines are not secure, or generate the Governor's voice telling millions of Californians their voting site has changed." Cal. Elec. Code § 20051(b); *see also id.* § 20012(a)(2).

30. The Legislature found that "candidates and parties are already creating and distributing deepfake images and audio and video content." Cal. Elec. Code §§ 20012(a)(3), 20511(c).

31. The Legislature found that "[v]oters will not know what images, audio, or video they can trust" due to deepfakes and disinformation. Cal. Elec. Code §§ 20012(a)(1), 20511(a).

32. The Legislature found that deepfakes and disinformation "can skew election results" and "undermine trust in the ballot counting process." Cal. Elec. Code §§ 20012(a)(3), 20511(c).

Dated: March 7, 2025

Respectfully submitted,

ROB BONTA
Attorney General of California
ANYA M. BINSACCA
Supervising Deputy Attorney General

/s/ Kristin A. Liska

KRISTIN A. LISKA
Deputy Attorney General
Attorneys for Defendants